



Task 10. «Linear subspaces»

For constructing a new secret sharing scheme Mary has to solve the following task on binary vectors. Let n be an integer number, $n \geq 2$. Let $\mathbb{F}_2^{2^n}$ be a 2^n -dimensional vector space over \mathbb{F}_2 , where $\mathbb{F}_2 = \{0, 1\}$ is a prime field of characteristic 2.

Do there exist subsets L_1, \dots, L_{2^n+1} of $\mathbb{F}_2^{2^n}$ such that the following conditions hold

1. L_i is a linear subspace of dimension n for every $i \in \{1, \dots, 2^n + 1\}$;
2. $L_i \cap L_j = \{\mathbf{0}\}$ for all $i, j \in \{1, \dots, 2^n + 1\}$, $i \neq j$;
3. $L_1 \cup \dots \cup L_{2^n+1} = \mathbb{F}_2^{2^n}$?

If «yes», show how to construct these subspaces for an arbitrary integer n .

Remark I. Recall several definitions and notions. Each element $x \in \mathbb{F}_2^k$ is a binary vector of length k , i. e. $x = (x_1, \dots, x_k)$, where $x_1, \dots, x_k \in \mathbb{F}_2$. For two vectors x and y of length k their sum is $x \oplus y = (x_1 \oplus y_1, \dots, x_k \oplus y_k)$, where \oplus stands for XOR operation. Let $\mathbf{0}$ be the zero element of the vector space, i. e. vector with all-zero coordinates. A nonempty subset $L \subseteq \mathbb{F}_2^k$ is called a *linear subspace* if for any $x, y \in L$ it holds $x \oplus y \in L$. It is easy to see that zero vector belongs to every linear subspace. A linear subspace L of \mathbb{F}_2^k has *dimension* n if it contains exactly 2^n elements.

Remark II. For example the case $n = 2$ we consider together. In the vector space \mathbb{F}_2^4 we can choose the following 5 required subspaces:

$$L_1 = \{(0000), (0001), (1110), (1111)\};$$

$$L_2 = \{(0000), (0010), (1001), (1011)\};$$

$$L_3 = \{(0000), (0011), (0100), (0111)\};$$

$$L_4 = \{(0000), (0101), (1000), (1101)\};$$

$$L_5 = \{(0000), (0110), (1010), (1100)\}.$$